Polyalphabetic Ciphers: Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.

The general name for this approach is **polyalphabetic substitution cipher**. All these techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenère Cipher: The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a.

The encryption formula is defined as

$$Ci = Ek(Pi) = (Pi + Ki \bmod m) \bmod 26$$

While the decryption formula is

$$Pi = Dk(Ci) = (Ci - Ki \bmod m) \bmod 26$$

where m is the length of the key string.

Example: Using the Vigenère ciphering method to encrypt this plaintext "**we are discovered save yourself**" by using "**deceptive"** as a keyword?

Solution:

Key: deceptivedeceptivedeceptive

Plaintext: wearediscoveredsaveyourself

Expressed numerically, we have the following result.

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

ciphertext: ZIC**VTW**QNGRZG**VTW**AVZHCQYGLMGJ

The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword. Thus, the letter frequency information is obscured.

Security of Vigenere Cipher:

1. Much more secure than Caeser cipher.
2. Need to determine key size.
3. Repetitions in ciphertext give clues to period.

Autokey system:

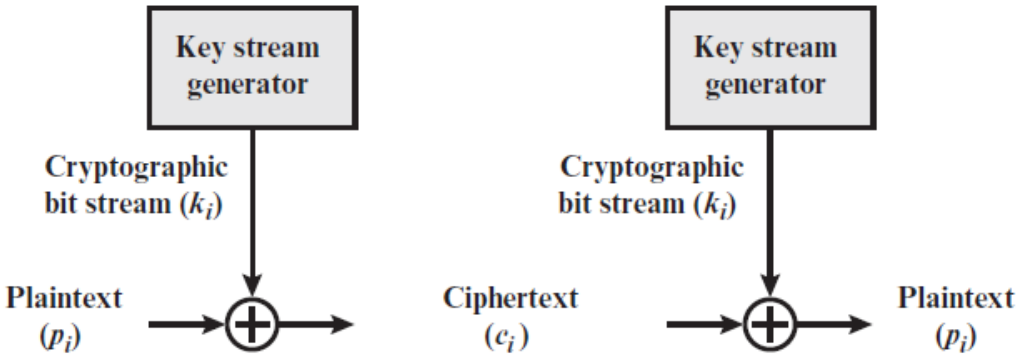
The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself. Vigenère proposed what is referred to as an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key. For our example,

Key: deceptivewearediscoveredsav

Plaintext: wearediscoveredsaveyourself

Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

Vernam cipher: The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named **Gilbert Vernam in 1918**.



His system works on binary data (bits) rather than letters. The system can be expressed succinctly as follows:

$$c_i = p_i \oplus k_i$$

where

p_i = ith binary digit of plaintext

k_i = ith binary digit of key

c_i = ith binary digit of ciphertext

$\oplus$ = exclusive or (XOR) operation

Decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

The essence of this technique is the means of construction of the key. Vernam proposed the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword. Although such a scheme, with a long

key, presents formidable cryptanalytic difficulties, it can be broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.

Example: Using Vernam ciphering method to encrypt the plaintext "**DOG**" using the key "**CAT**"?

Solution: From ASCII code

Plaintext	D	O	G
Binary Form of Plaintext	01000100	01001111	01000111
Key	C	A	T
Binary Form of key	01000011	01000001	01010100
Binary Form of Ciphering	00000111	00001110	00010011

One-Time Pad

Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a **random key** that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt **a single message**, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a one-time pad, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

The encryption formula is defined as

$$Ci = Ek(Pi) = (Pi + Ki) \bmod 26$$

While the decryption formula is

$$Pi = Dk(Ci) = (Ci - Ki) \bmod 26$$

Example: Encrypt the plaintext "**MEET ME OUTSIDE**" using the key "**BDUFGHWEIUFGW**"?

Solution:

Plaintext	M	E	E	T	M	E	O	U	T	S	I	D	E
Numerical Plaintext	12	4	4	19	12	4	14	20	19	18	8	3	4
Key	B	D	U	F	G	H	W	E	I	U	F	G	W
Numerical key	1	3	20	5	6	7	22	4	8	20	5	6	22
Numerical Ciphertext	13	7	24	24	18	11	10	24	1	12	13	9	0
Ciphertext	N	H	Y	Y	S	L	K	Y	B	M	N	J	A

The security of the one-time pad is entirely due to the randomness of the key. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Transposition cipher: In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a **permutation** of the plaintext. That is, the order of the units is changed.

Rail Fence cipher: The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows.

For example, using depth of three (**three row**) "rails" and a message of "**WE ARE DISCOVERED FLEE AT ONCE**", the cipherer writes out:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Then reads off:

WECRL TEERD SOEEF EAOCA IVDEN

Homework: Using the Rail Fence method to cipher the text "**Thank you very much**" using depth of three?

Row Column Transposition Ciphering:

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a **keyword**.

For example, the word **ZEBRAS** is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "**6 3 2 4 1 5**".

In a regular columnar transposition cipher, any spare spaces are filled with nulls. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword **ZEBRAS** and the message **WE ARE DISCOVERED. FLEE AT ONCE**. In a regular columnar transposition, we write this into the grid as:

Key	Z	E	B	R	A	S
Order	6	3	2	4	1	5
Plaintext	W	E	A	R	E	D
	I	S	C	O	V	E
	R	E	D	F	L	E
	E	A	T	O	N	C
	E	**Q**	**K**	**J**	**E**	**U**

Providing five nulls (QKJEU) at the end. The ciphertext is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

In the irregular case, the columns are not completed by nulls:

Key	Z	E	B	R	A	S
Order	6	3	2	4	1	5
Plaintext	W	E	A	R	E	D
	I	S	C	O	V	E
	R	E	D	F	L	E
	E	A	T	O	N	C
	E					

This results in the following ciphertext:

EVLNA CDTES EAROF ODEEC WIREE

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length. Then he can write the message out in columns again, then re-order the columns by reforming the key word.

Double transposition:

A single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.

As an example, we can take the result of the irregular columnar transposition in the previous section, and perform a second encryption with a different keyword, STRIPE, which gives the permutation "564231":

Key	S	T	R	I	P	E
Order	5	6	4	2	3	1
Plaintext	E	V	L	N	A	C
	D	T	E	S	E	A
	R	O	F	O	D	E
	E	C	W	I	R	E
	E					

As before, this is read off column wise to give the ciphertext:

CAEEN SOIAE DRLEF WEDRE EVTOC

If multiple messages of exactly the same length are encrypted using the same keys, they can be anagrammed simultaneously. This can lead to both recovery of the messages, and to recovery of the keys (so that every other message sent with those keys can be read).

Classical Ciphers: Usefulness and Security:

- Polyalphabetic ciphers and transposition ciphers are stronger than simple substitution ciphers. However, if the key is short and the message is long, then various cryptanalysis techniques can be applied to break such ciphers.

- Classical ciphers, even simple substitution ciphers can be secure in a *very strong sense* if the use of cryptographic keys follows certain conditions. In fact, with the proper key usages, simple substitution ciphers are widely used in cryptographic systems and protocols.

Homework: Using irregular double transposition method to decipher the ciphertext "**CAEEN SOIAE DRLEF WEDRE EVTOC**" using keyword 1= ZEBRAS and keyword 2= STRIPE?